UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,382	02/13/2004	Graham A. Wheeler	50037.219US01	9021

27488 7590 03/12/2007

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
MEDE, ESTEVE	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,382	WHEELER, GRAHAM A.	
	Examiner	Art Unit	
	Esteve Mede	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claim Objections

1. Claim 1, 10-12, 14 are objected to because of the following informalities: in claim 1, line 3-4 the term 'transmission in the next frame" should be –transmission in another frame--; in claim 1, line 10 the term "the hash key" should be --the selected hash key--; in claim 1 line 11 the term "computing an HMAC value" should be –computer a keyed-hash message authentication code (HMAC) value--; in claim 10, line 2 and 14, line 2 the term "a time step" should be --a time stamp--; in claim 12, line 4 the term "a time step" should be --a time stamp--; in claim 11, line 3 the term "receiving an RSA signed datum" should be –receiving Ron Rivest, Adi Shamir and Leonard Adleman (RSA) signed datum in claim 11, line 4 the term "an RSA" should be --the RSA--. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. **Claim 1-10 and 19** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1, as claimed the phrase "and assembling the next frame such that the data block and the HMAC value appear before the hash key in the frame transmission" is confusing ass it cannot be ascertained because the specification fails to disclose how the HMAC value appears before the hash key.

the specification doesn't provide any details how one of ordinary skilled in the art can achieve such limitation, therefore the entire claim 1 is rejected, as well as its dependent claims 2-10.

Claim 1, the phrase retrieving a data block that is scheduled for transmission in the next frame" is confusing

Claim 1, the phrase "selecting a hash key that is associated with the data block" is confusing, because in claim 1, line 3 the applicant refers to a single data block, in claim 1, line 6 the applicant refers to multiple data blocks, therefore it is unclear as to which "data block: applicant referring to in the claimed invention.

Claim 8, as claimed "wherein periodically signing the datum comprises at least one of signing the datum for every frame, and signing the datum over an interval that does not correspond to every frame" the claimed invention as claimed is confusing as the specification failed to disclose how the datum is signed for every frame and then signed the datum not corresponding to every frame. No further merit will be giving to this claim.

Claim 19, as claimed " a means for recording the other hash key when the frame is accepted, wherein the other hash key is utilized for verification of subsequently received transmission frames" the term "recording the other hash" cannot be ascertained because the specification fails to disclose how the recording of the other hash is being done.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. **Claims 11 and 16** are rejected under 35 U.S.C. 102(e) as being anticipated by Carro (US 2004/0054906 A1).

Regarding claim 11, Carro discloses a method for authenticating frame transmission from a server to a client device, comprising; retrieving signed data from a frame (para. 0032, lines 7-9); verifying an RSA signature associated with the RSA signed datum from the frame (para. 0032, lines 9-12); storing a hash key that is associated with the frame when the RSA signature is verified (the prior art discloses the hash key of the hash function received is being computed to obtain the hash value, therefore, the hash key must have be stored before it can use to decode the hash value (0032, lines 13-18); retrieving another hash key and an HMAC value from the frame; verifying the other hash key (a frame is a data packet of fixed variable, and since every frame transmitted is hashed in iteration sequence each frame must be check and verified for the hash key. the limitation of retrieving another hash key and an HMAC value from the frame and

verifying the key is an intrinsic property of the claim invention); verifying the HMAC value with the other hash key (para. 0032, lines 11-20); discarding the frame when at least one of the other hash key and the HMAC value fail verification (para. 0032, lines 21-24); accepting the frame when the other hash key and the HMAC value are successfully verified (para. 0032, lines 18-21).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1-10, and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mache (US 2001/0002929 A1).

Regarding claim 1 Mache discloses a method for signing transmission from a broadcast server to a client comprises; receiving a data block that is scheduled for transmission in the next from (para. 0016, lines 1-2; 0037, lines 1-2); selecting a secret key that is associated with the client device for a number of data blocks (para. 0014, lines 3-6; para. 0017, lines 3-5); computing a set of hash keys using the secret key and a count that is associated with time (para. 0031, lines 1-4; para. 0036, lines 1-4); computing an HMAC value for the next frame using the selected hash key (para. 0037, lines 6-7; in the prior art communication are taking place using HMAC for every packets so as to maintain security of the

communication exchange); periodically signing and transmitting a datum containing the hash key of an earlier or initial frame with a digital signature key (para. 0037, lines 1-4) Mache discloses all the limitations as disclosed above; except for assembling the next frame such that data block and the HMAC value appear before the hash key in the frame. The general concept of having the HMAC value appear before the hash key as recited in claim 1 is well known in the art, It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Mache to include the use of having the HMAC value appear before the hash key in his advantageous system, as configuring packet header is a common and everyday occurrence throughout the Cryptography and Information Security art and configuring the packet to have the HMAC appear before the hash would have been an obvious matter of design preference, base on such common factor as the secret key must be use to calculate the HMAC; the ordinarily skilled artisan choosing the best method which would most optimize the cost and performance of the device for a particular application at hand, based upon the above noted common design criteria.

9. **Claims 1-10, and 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mache (US 2001/0002929 A1).

Regarding claim 2 all the limitation of claim 2 is met as stated above except that wherein the datum corresponds to at lest one of (n, S)} k and (n, b, S) where b corresponds to a preceding frame number from a previous frame transmission. The general concept of the data corresponds to at least one

preceding frame number from a previous frame transmission is well known in the art as illustrated by Ellison, which discloses transmission of multiple packets using sequence number generator (para. 0034, lines 1-6; para. 0033, lines 6-9). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Mache to include the use of a number sequence in order to compare frames that were previously received with current received frames, thus that replay attack can be avoided.

Regarding claim 3, Mache meets all the limitation of claim 3 as disclosed above except that, the method comprising, selecting the count such that the count is associated with an index of the data block. The general concept of selecting the count such that the count is associated with an index of the data block is well known in the art as illustrated by Ellison, which discloses the increments of a sequence number (para. 0033, lines 6-8; the prior art does not use the term count associated with an index, however the incremented sequence number is doing exactly the same function as the count associated with an index). Therefore it would have been obvious for one of ordinary skill in that art at the time of the invention to modify Mache to include the use of incremented sequence number in order to verify the sequence in which the frames are arriving, so that the receiving unit may know which frame to expect next in the transmission.

Regarding claim 4, Mache discloses the method, comprising selecting the count hash such that the count corresponds to a time stamp associated with

an internal clock in the broadcast server (para. 0039, lines 3-4; para. 0025, lines 1-3).

Regarding claim 5, Mache discloses the method wherein computing the set of hash keys corresponds to applying a one-way function to the secret key (para. 0023, lines 4-7).

Regarding claim 6, The method of claim 1, wherein computing the HMAC value corresponds to a hashed message authentication code, wherein a value (H.sub.i) associated with the hashed message authentication code is given as H.sub.i=HMAC (F.sub.i, S.sub.i), where F.sub.i corresponds to the data being signed, S.sub.i the key for signing, and i the sequence number associated with the data and key (para. 0009, lines 1-9; para. 0086, lines 1-3; para. 0036, lines 1-4).

Regarding claim 7, Mache discloses the communicating parties share a secret key, which can securely exchange periodically (para. 0037, lines 1-3).

Regarding claims 9-10, Mache discloses all the limitation of claim 9 except that the method comprising, incrementing the count before retrieving a data block that is scheduled for transmission in the next frame. The general concept of incrementing the count before retrieving a block of data is well know in the art as illustrated by Ellison, which discloses an incremented count of the data block (para. 0046, lines 8-11); therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Mache to include the use of increment count of data block in order to sensory elements for the verify to check, so that the message can be protected against attack.

10. **Claims 12-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over Carro (US 2004/0054906 A1) in view of Mache (US 2001/0002929 A1).

Regarding claims 12-14, Carro discloses all the limitation of claim 12 except that the method further comprising a count associated with the client device; computing a hash key using the count and a secret key that is known by both the server and the client; wherein the count corresponds to at least on of a time step in the client device; identifying the frame number associated with the frame. The general concept of evaluating a count associated with the client device, computing a hash key using the count and a secret key that is known by the server and the client, wherein the count corresponds to at least one of a time stamp in the client device identifying the frame number associated with the frame, and identifying the block number that is associated with the frame is well known in the art as illustrated by Mache, which discloses a secure random number generator to be used among the communication parties (para. 0036, lines 1-4); computing a hash key using the count and a secret key that is known by the server and the client (para. 0037, lines 1-2); wherein the count corresponds to a time stamp in the client device (para. 0021, lines 1-4); identifying the frame number associated with the frame (para. 0020, lines 6-8); and identifying the clock number associated with the frame (identifying the block number and frame are intrinsic property of the claim invention, as if the claim invention fails to identify the sequence of the frame it is to received security of the data will be lost. Therefore, it would have been obvious for one of ordinary

skill in the art at the time of the invention to modify Carro, to include the use of Mache in order to check packets received from the sender have not been modified, out of sequence and with the time interval set by the communication parties.

Regarding claim 13, Carro discloses all the limitation of claim 13 except that, retrieving a count in the client device, computing an expected hash key from the previous stored hash key and the count, The general concept of retrieving a count in the client device, computing an expected hash key from the previous stored hash key and the count is well known in the art as illustrated by Mache, which discloses a generator to produce random number (count) on the frames (para. 0036, lines 1-4); therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Carro to include the use of a count in order to compare the hash key and the sequence number, so that validity of the message can be check.

Regarding claim 14, the prior art disclosed the entire limitation claim 14, in claim 12.

Regarding claim 15, Carro discloses the method wherein verifying the HMAC value with the other hash key comprising, computing a (H) associated with a hash message authentication code for a given H=HMAC (para 0027, lines 1-5; para 0032 lines 1-24; para. 0028, lines 4-8), when F corresponds to the data being signed, S the key for signing, an comparing the computed value with the retrieved HMAC value from the frame (para. 0032, lines 16-20); except that *i* is the sequence number associated with the data and key. The general concept

of a letter being the sequence number associated with the data and key is well known in the art as illustrated by Mache, which discloses a number generator to generate sequence of random number (0036, lines 1-4). Therefore it would have be obvious for one of ordinary skill in the art at the time of the invention to modify Carro to include the us of a sequence number in order to associate a number with a message or key.

Regarding claims 18 and 20, Carro discloses the broadcast communication system further comprising, a broadcast receiver in the client device that is arranged to receive a transmitted frame (para. 0005, lines 5-7); wherein the transmitted frame starts with another HMAC value (in the prior are all the frames use HMAC value, para. 0006); continue with another signed data followed by another block, and ends with another hash key (intrinsic properties of the frame transmission when there are more then one frame); a hash function of the client device that is arranged to compute additional hash keys (para. 0032, lines 11-12) for the frame transmission count, the secret key (para. 0027, lines 7-11); a verification block of the client device that is arranged to verify the other hash key with the other hash key and verify the HMAC value (para. 0032, lines 12-20); a means for discarding the frame in the client device when at least one of the other hash key and the HMAC value fail verification (para. 0032, lines 21-24); and a means for accepting the frame in the client device when the other hash key and the HMAC value are successfully verified (para. 0032, lines 18-20); however Carro does not disclosed that a counter in the client device that is arranged to provide another count, and a hash function in the client device that

is arranged to compute additional hash keys using the count and previously stored hash keys (storing a hash key that is associated with the frame when the RSA signature is verified (the prior art discloses the hash key of the hash function received is being computed to obtain the hash value, therefore, the hash key must have be stored before it can use to decode the hash value). The general concept of the client device arranged to provide another count, the hash function ready to compute additional hash keys using the count is well known in the art as illustrated by Mache, which discloses a number generator to generate count (para. 0036, lines 1-4). Therefore, it would have been obvious for one of ordinary skill in the art at the time at the time of the invention to Carro to include the use of a random number generator in order to provide a sequence of random number (count), which to be use with the hash key, so that it would be difficult for a replay attack.

11. **Claim 19** is rejected under 35 U.S.C. 103(a) as being unpatentable over Carro (US 2004/0054906 A1) in view of Mache (US 2001/0002929 A1) and further in view of Ellison et al. (US 2004/002501 A1).

Regarding claim 19, the prior art meet all the limitation of claim 18, except that the broadcast communication further comprising, a means for recording the other hash key when the frame is accepted; however the general concept of a means for recording the other hash key when the frame is accepted is well known in the art as illustrated by Ellison, which discloses a CD-ROM (para. 0034, lines 9-10); therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Carro and Mache to

include a recording means in order to record keys that have been accepted while waiting for other frame, and use the recorded keys to check the validation of the frames.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esteve Mede whose telephone number is 571-270-1594. The examiner can normally be reached on Monday thru Friday, 8:30-5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-6681. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Esteve Mede
em
February 28, 2007

FRANTZ JULES
SUPERVISORY PATENT EXAMINER